June 25, 2018
Mizuho Financial Group, Inc.

Establishment of Cybersecurity Management Declaration

Mizuho Financial Group, Inc. (President & Group CEO: Tatsufumi Sakai) and our group companies[1] have established a *Cybersecurity Management Declaration* taking into consideration the *Keidanren Cybersecurity Management Declaration* released by the Japan Business Federation (Keidanren) in March 2018.

In order to realize Society 5.0[2], Keidanren has put forward various proposals to reinforce cybersecurity measures, such as actions to be taken by the public and private sectors, including information sharing and training personnel. In light of this, the *Keidanren Cybersecurity Management Declaration* broadly shares the purpose of the cybersecurity measures and sets forth the importance of accelerating collaborative efforts among all types of stakeholders in the business community.

Keidanren's initiatives have helped raise our awareness of the importance of cybersecurity measures. We have therefore formulated a strategy under which we have made cyberattack prevention a top management priority. With Mizuho's Cyber Incident Response Team taking the lead, we have assigned cybersecurity professionals to this task and are drawing on intelligence and cutting-edge technology developed through partnerships with external specialized agencies, while also taking initiatives to strengthen our strategic resilience capabilities[3], which include monitoring via an integrated Security Operation Center, analyzing computer viruses, developing multilayer defense systems, and other measures.

In consideration of Mizuho's vital role within the social infrastructure as a financial institution, we are proactively implementing cybersecurity measures and doing our part to contribute to building a safe and secure cyberspace environment under our *Cybersecurity Management Declaration*.

1: Mizuho Bank, Ltd., Mizuho Trust & Banking Co., Ltd., Mizuho Securities Co., Ltd., Asset Management One Co., Ltd., Mizuho Research Institute Ltd., Mizuho Information & Research Institute, Inc., Mizuho Private Wealth Management Co., Ltd., Trust & Custody Services Bank, Ltd.

2: Society 5.0 is a major policy promoted by the Japanese Cabinet Office's Council for Science, Technology and Innovation for creating a "Super Smart Society" (Society 5.0) through advances in science and technology.

3: To ensure business continuity, emphasize early response/recovery to prevent damage from spreading.

1. Recognize Cybersecurity as a Management Issue
   - Enhance their own understanding of the latest cybersecurity developments and actively engage in management by positioning cybersecurity spending as an investment.
   - Take personal responsibility for cybersecurity measures while recognizing that cybersecurity is a critical management issue, confronting realities, addressing risks, and exercising leadership.

Cyberattacks are a top-priority management issue for our organization from the perspective of ensuring uninterrupted provision of services for our customers as well as maintaining stable operations and the sustainable growth of our financial infrastructure. Management discusses cybersecurity risks on a regular basis, allocating resources for managing them and taking action to strengthen our security framework.

2. Develop Management Policies and Declare Intentions
   - Develop management policies and business continuity plans aimed at prompt recovery from security incidents while prioritizing detection, response, and restoration in addition to identifying and protecting against risks.
   - Take the lead in declaring companies' intentions to internal and external stakeholders and make every effort to voluntarily disclose recognized risks, and measures to deal with them, in corporate reporting.

Mizuho, led by our Cyber Incident Response Team, works to strengthen our strategic resilience capabilities through measures such as conducting monitoring via an integrated SOC (security operations center), analyzing computer viruses, and developing and deploying multilayer defense systems.

We believe it is important to keep our customers updated about the efforts we are making to strengthen our cybersecurity, so going forward we will be disclosing this information in our Integrated Report and on our website.

3. Build Internal and External Systems and Implement Security Measures
   - Ensure sufficient resources including budgets and personnel, establish internal systems, and take necessary HR, technical, and physical measures.
   - Develop human resources and conduct training required for those at every level, including managers, corporate planning staff, technical specialists, and other employees.
   - Manage cybersecurity throughout domestic and international supply chains, including business partners and outsourcing contractors.

We acknowledge that cultivating a professional workforce with high-functioning knowledge of cybersecurity is an important medium- to long-term task for Mizuho. We are working with outside experts to develop our workforce and motivate our employees in this direction.
By conducting training at every personnel level and participating in cross-industry exercises, we are also enhancing the effectiveness of our internal frameworks and procedures.
We strive to ensure the integrity of our supply chain by monitoring cybersecurity at our contractors and business partners.

4. Contribute to Widespread Use of Cybersafe Products, Systems, and Services
   - Manage cybersecurity across the full spectrum of corporate activity, including development, design, production, and supply of products, systems, and services.

We undertake a wide range of cybersecurity countermeasures to protect our customers' assets from criminal activity. In terms of internet banking, these measures include providing security software for our customers, optimizing verification systems, and monitoring transactions.
Through our website and other mediums, we also send notifications regarding potential password exploitation and virus infections to ensure the safety of our services.

5. Contribute to Building Safe and Secure Ecosystems
   - Collaborate with relevant government agencies, organizations, industry associations, and other bodies to actively share information, engage in dialogue, and build human networks, both in Japan and internationally.
   - Contribute to reinforcement of cybersecurity throughout society by raising awareness of measures taken on the basis of such information.

In the closely-connected world in which we live, we believe it is important to further optimize coordination between social institutions, both in times of crisis and in times of stability. That is why we are constantly working to create and maintain reliable communication and information-sharing structures regarding cybersecurity with government institutions, regulatory authorities, law enforcement agencies, the Financial Services Information Sharing and Analysis Center, and the Financials ISAC Japan.
We proactively share the information we glean from research and analysis with external parties in order to benefit society at large.